UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,213	04/09/2001	Mototsugu Nishioka	501.39942X00	8046

20457 7590 08/24/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/828,213	Applicant(s) NISHIOKA ET AL.
	Examiner Eleni A Shiferaw	Art Unit 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-47 are presented for examination.

Claim Objections

2. Claim 22 is objected to because of the following informalities: claim 22 on page 39 lines 12, "}" is unclear where it is opened. Appropriate correction is required.

3. Claim 25 is objected to because of the following informalities: claim 25 on page 41 lines 5, "}" is unclear where it is opened. Appropriate correction is required.

4. Claim 27 is objected to because of the following informalities: claim 27 on page 43 lines 12, "}" is unclear where it is opened. Appropriate correction is required.

5. Claim 34 is objected to because of the following informalities: claim 34 on page 46 lines 21-24, "(pi, β) (1<= x(sub (i)) = C^(((p(sub i)+1) β)/4) mod p(sub i) i<=h)" is unclear, where i is between 1 and h. Appropriate correction is required.

6. Claim 39 is objected to because of the following informalities: claim 39 on page 48 lines 9, "creating m1,p and m1,q by" unfinished sentence. Appropriate correction is required.

7. Claim 40 is objected to because of the following informalities: claim 40 on page 48 lines 19, "creating m1,p and m1,q by" unfinished sentence. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 22-28, 29-31, 33-38, and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention because

on Fig. 7-9 symbol "⊕ " is used x=(m0^(k1) ⊕ G(r))||(r ⊕ H(m0^(k1) ⊕ G(r)))

on the claims 22-28, 29-31, 33-38, and 40 symbol "⊙ "is used, they are different symbols with different meanings. Appropriate correction is required.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-2, 4-5, 9-11, 32, 39, 41-42, and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent 4,405,829) in view of Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999).

11.1 As per claim 1, Rivest teaches the communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising:

a key generating step of generating a secret key (p, q, β) satisfying

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β ϵ Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

and

- n = p^d q . (d > 1 is odd.)

- k : binary length of pq
- $\alpha \in Z$,

a public key (n, k, α) satisfying (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

from the ciphertext (C, a), and regarding as the plaintext m any of Φ(m(sub1, p), m(sub 1, q)), Φ(-m(sub1, p), m(sub 1, q)), Φ(m(sub1, p), -m(sub 1, q)), and Φ(-m(sub1, p), -m(sub 1, q)), that satisfies (x/n)=a and 0<x<2^(k-2), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more primes);

Rivest do not explicitly teach encrypting step performed by the sender device, of

C = m^(2nα) mod n;

Jacobi's symbol a=(m/n); and

receiver device, of using the receiver's secret key (p, q, β) to compute

m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p,

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q,

However Crepeau NPL teaches: (1) an encrypting step performed by the sender device, of C = m^(2nα) mod n (Crepeau NPL, page 10, 1.11) computing

for plaintext m (0 < m < 2^(k-2)), computing Jacobi's symbol a=(m/n), and sending ciphertext (C,a) to the receiver device (Crepeau NPL, Page 5-6, 1.5); and

(2) a decrypting step performed by the receiver device, of using the receiver's secret key (p, q, β) to compute

m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9),

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Crepeau NPL with in the system of Rivest because it would speed up the calculation when enciphering and deciphering. It is obvious to compute m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p, and m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q, from C = m^(2nα) mod n when using three prime numbers because Crepeau NPL teaches if p Ξ 3 (mod 4) is prime, then the solutions to x^2 Ξ a (mod p) are r = a^(p+1)/4 mod p; to proof, (a^(p+1)/4)^2 Ξ a^(p-1).a (mod p) Ξ a (mod p) (Claude NPL, page 9-10). Therefore it is obvious to have an encryption step performed by the sender device when using three prime numbers, of C = m^(2nα) mod n and compute a decryption step performed by the receiver device, of using the receiver's secret key (p, q, β) to compute m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p, and m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q because it speeds up calculation when breaking things up.

11.2 As per claim 4, Rivest teaches a communication system using public key cryptosystem in which a sender device encrypts send data by using a receiver's public key, the system comprising:

(a) a sender device comprising:

a key generating device for generating a secret key (p, q, β)

satisfying

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β ϵ Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

and

- n = p^d q . (d > 1 is odd.)
- k : binary length of pq
- α ϵ Z,
- a ϵ {-1, 1},

a public key (n, k, α , a) (k is the bit length of pq) satisfying } (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

a communication device for sending ciphertext C to the receiver device (Rivest, Col. 4 lines 56-67);

a device using the receiver's secret key (p, q, β) to compute from the ciphertext C (Rivest Col. 4 lines 14-32, Rivest Col. 13 lines 29-34); and

a device regarding as the plaintext m any of Φ(m(sub1, p), m(sub 1, q)), Φ(-m(sub1, p), m(sub 1, q)), Φ(m(sub1, p), -m(sub 1, q)), and Φ(-m(sub1, p), -m(sub 1, q)), that satisfies (x/n)=a and 0<x<2^(k-2), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more primes);

Rivest do not explicitly teach a device for computing

C = m^(2nα) mod n,

Jacobi's symbol a=(m/n), and

a receiver device comprising: m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p,

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q,

However Crepeau NPL teaches a device for computing

C = m^(2nα) mod n (Crepeau NPL, page 10, 1.11),

for plaintext m satisfying a=(m/n) (0 < m < 2^(k-2)) (a=(m/n denotes Jacobi's symbol; and a communication device for sending ciphertext C to the receiver device (Crepeau NPL, Page 5-6, 1.5); and

(b) a receiver device comprising:

m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9),

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Crepeau NPL with in the system of Rivest because it would speed up the calculation when enciphering and deciphering. It is obvious to compute m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p, and m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q, from C = m^(2nα) mod n when using three prime numbers because Crepeau NPL teaches if p ≡ 3 (mod 4) is prime, then the solutions to x^2 ≡ a (mod p) are r = a^(p+1)/4 mod p; to proof, (a^(p+1)/4)^2 ≡ a^(p-1).a (mod p) ≡ a (mod p) (Crepeau NPL, page 9-10). Therefore it is obvious to have an encryption step performed by the sender device when using three prime numbers, of C = m^(2nα) mod n and compute a decryption step performed by the receiver device, of using the receiver's secret key (p, q, β) to compute m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p, and m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q because it speeds up calculation when breaking things up and using Jacobi's symbol makes easy and efficient calculation.

11.3 As per claim 2, Rivest and Crepeau NPL teach all the subject matter as described above.

In addition Rivest teaches the communication method using public key cryptosystem, comprising the step of: generating and publicizing the public information (n, k, α) by the receiver device (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34).

11.4 As per claim 5, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches the communication system using public key cryptosystem according to Claim 4, wherein the receiver device comprises a device for creating the public information (n, k, α , a) (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34).

11.5 As per claim 9, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem, comprising the step of transforming message text to be sent to the receiver from the sender into plaintext m whose contents are provided with predetermined redundancy, and encrypting the plaintext m by the method described in Claims 1 or 4, wherein the receiver device decrypts the plaintext m by the method described in Claims 1 or 4 and checks the predetermined redundancy (Rivest Col. 6 lines 4-37, abstract).

11.6 As per claim 10, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem, comprising the step of transforming message text to be sent to the receiver from the sender into plaintext m whose contents are provided with a predetermined, meaningful message, and encrypting the plaintext m by the method described in Claims 1 or 4, wherein the receiver device decrypts the plaintext m by the method described in Claims 1 or 4 and checks the contents of the predetermined, meaningful message (Rivest Col. 6 lines 4-37, abstract).

11.6 As per claims 11 and 47, Rivest and Crepeau NPL teach all the subject matter as described above.

In addition Rivest teaches the communication method using public key cryptosystem, wherein the value of d (d>1) is variable (Rivest Col. 4 lines 56-col. 5 lines 17).

11.7 As per claim 32, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Crepeau NPL teaches an encryption method according to Claim 1, for computing ciphertext C in two different devices, comprising the steps of:

$C = x^{(2\alpha)} \bmod n$ (Crepeau NPL, page 10, 1.11)

in a device 1, after computing outputting C1 to a device 2; and

$C = C1^{(n)} \bmod n$

in the device 2, by computing

computing the ciphrtext C (Rivest, Col. 5 lines 50-col. 6 lines 3). The motivation for combining are the same as claim 1 above.

11.8 As per claim 39, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Crepeau NPL teaches the communication method using public key cryptosystem according to Claim 1, comprising the step of:

creating ciphertext C by

$C = m^{(2\alpha)} \bmod n$ (Crepeau NPL, Page 10, 1.11)

and creating $m_{(1,p)}$ and $m_{(1,q)}$ by

$m_{(1,p)} = C^{(((p+1)\beta)/4)} \bmod p$ (Crepeau NPL, Page 9, 1.9),

$m_{(1,q)} = C^{(((q+1)\beta)/4)} \bmod q$ (Crepeau NPL, Page 9, 1.9) The rational for combining are the same as claim 1 above.

11.9 As per claim 41, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches a program product, comprising:

a program for instructing a computer to execute one of the key generating step, the encrypting step, and the decrypting step which are described in Claim 1 (Rivest, col. 6 lines 21-37); and

a medium embodying the program (Rivest, Col. 6 lines 48-57).

11.10 As per claim 42, Rivest and Crepeau NPL teach all the subject matter as described above. In addition, Rivest teaches a communication system using public key cryptosystem which comprises a sender device and a receiver device and in which the sender device encrypts send data using a receiver's public key (Rivest, Col. 2 lines 63-67),

wherein the receiver device, using an operation unit the receiver device has, executes the key generating step described in Claim 1 and generates the secret key (p, q, β) and the public key (n, k, α) (Rivest, Col. 13 lines 29-34),

wherein the receiver device, using the operation unit the receiver device has, executes the decrypting step described in Claim 1 and obtains plaintext m (Rivest, Col. 6 lines 21-37) and

wherein the sender device, using an operation unit the sender device has, executes the encrypting step described in Claim 1, computes Jacobi's symbol a=(m/n), and sends ciphertext (C, a) to the receiver device (Crepeau NPL, page 5-6, 1.5) The rational for combining are the same as claim 1 above.

11.11 As per claim 45, Rivest, and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches the communication system using public key cryptosystem according to Claim 4,

wherein the device of the sender device to encrypt the plaintext m provides predetermined redundancy to the message text to be sent to the receiver and produces the contents of the resulting message text as the plaintext m (Rivest, Col. 6 lines 4-37, abstract) and

wherein the device of the receiver device to decrypt the plaintext m checks the predetermined redundancy (Rivest, Col. 6 lines 4-37, abstract).

11.12 As per claim 46, Rivest and Crepeau NPL teach all the subject matter as described above. In addition, Rivest teaches the communication system using public key cryptosystem according to Claim 4,

wherein the sender device comprises the step of providing a predetermined, meaningful message to the message text to be sent to the receiver and producing the contents of the resulting

message text as the plaintext m, and encrypting the plaintext m by the method described in Claim 4 (Rivest, Col. 6 lines 4-37, abstract), and

wherein the receiver device comprises the step of decrypting the plaintext m by the method described in Claim and checking the contents of the predetermined, meaningful message (Rivest, Col. 6 lines 4-37, abstract).

12. Claims 3, 6, 8, 12-17, 19, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent 4,405,829) in view of Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), and in further view of Kocher et al. (Kocher, U.S. Patent No. 6,289,455 B1).

12.1 As per claim 12, Rivest and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches the method by which a sender device performs cipher communications by using a receiver's public key, the method comprising key generating steps of:

generating a secret key (p, q, β) satisfying

- p, q : prime integers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in Z$, $\alpha \beta \equiv 1$ (mod lcm $(p - 1, q - 1)$)

a public key (n, k, α) (k is the bit length of pq) satisfying

- n = p^d q . (d > 1 is odd.)
- k : binary length of pq
- $\alpha \in Z$,

f : one-way function (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

from the ciphertext (C, a), computing as the send data m any of Φ(m(sub1, p), m(sub 1, q)), Φ(-m(sub1, p), m(sub 1, q)), Φ(m(sub1, p), -m(sub 1, q)), and Φ(-m(sub1, p), -m(sub 1, q)), that satisfies (x/n)=a and 0<x<2^(k-2), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more) The motivation for combining are the same as claim 1 above;

(1) in the sender device C = m^(2nα) mod n (Crepeau NPL, page 10, 1.11);

receiver device, for send data m (0<m<2^(k-2)), computing and computing Jacobi's symbol a=(m/n), sending ciphertext (C, a) to the receiver device (Crepeau NPL, page 5-6, 1.5);

(2) in the receiver device, using the receiver's secret key (p, q, β) to compute

m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Rivest and Crepeau NPL do not explicitly teach key sharing K=f(m),

However Kocher teaches key sharing using an RSA public key (Kocher Col. 26 lines 41-53)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Kocher with in the combination of Rivest and Crepeau NPL because it would help prevent key redistribution attacks that involve using key produced by one Cryptographic Rights Unit in many playback devices and it would decode the content if the Cryptographic Rights Unit has sufficient I/O bandwidth and computational speed (Kocher Col. 26 lines 41-53). It is obvious to employ the key sharing of Kocher with in the system of Rivest and Crepeau NPL because the teachings of Kocher would generate encryption or decryption key, and encrypt or decrypt the digital content and distribute it in encrypted form.

12.2 As per claim 15, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above.

In addition Rivest teaches a method by which a sender device performs cipher communications by using a receiver's public key, the method comprising key generating steps of:

generating a secret key (p, q, β) satisfying

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β є Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

and

- n = p^d q . (d > 1 is odd)
- k : binary length of pq
- α є Z,
- f : one-way function

a public key (n, k, α , a) (k is the bit length of pq) satisfying (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

from the ciphertext C, computing as the send data m any of Φ(m(sub1, p), m(sub 1, q)), Φ(-m(sub1, p), m(sub 1, q)), Φ(m(sub1, p), -m(sub 1, q)), and Φ(-m(sub1, p), -m(sub 1, q)), that satisfies (x/n)=a and 0<x<2^(k-2), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more prime numbers) The motivation for combining are the same as claim 1 above;

Crepeau NPL teaches:

(1) in the sender device, with the receiver device, for send data m (0<m<2^(k-2)) satisfying a=(m/n) (a=(m/n) denotes Jacobi's symbol) (Crepeau NPL, page 5-6, 1.5),

computing C = m^(2nα) mod n (Crepeau NPL, page 10, 1.11);

and

(2) in the receiver device, using the receiver's secret key (p, q, β) to compute

m(sub 1,p) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

m(sub 1,q) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Kocher teaches key sharing, K=f(m), using an RSA public key (Kocher Col. 26 lines 41-53) The rational for combining are the same as claim 12 above.

12.3 As per claims 3, and 6 Rivest and Crepeau NPL teach all the subject matter as described above.

Rivest and Crepeau NPL do not explicitly teach deleting α = β =1, α and β from the public key and the secret key, respectively

However Kocher teaches key deletion that reads on the communication method (system) using public key cryptosystem, wherein, for α = β =1, α and β are deleted from the public key and the secret key, respectively (Kocher Col. 25 lines 43-58).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Kocher with in the combination of Rivest and Crepeau NPL because it would ensure content providers that unauthorized users who have lost their authorization can not access content (Kocher Col. 25 lines 43-58). Key deletion is important because when a user terminates a subscription, a password (rights key) given to a user needs to be deleted by the content providers. Otherwise the users who have lost their authorization can access content after termination.

12.4 As per claim 8, Rivest and Crepeau NPL teach all the subject matter as described above.

Rivest and Crepeau NPL do not explicitly teach including check information for checking whether message text to be sent to the receiver from the sender has been correctly decrypted,

However Kocher teaches a checksums in a secure cryptographic rights unit (Kocher, Col. 28 lines 1-4) that reads on the communication method using public key cryptosystem, comprising the step of creating the plain text m so as to include check information for checking whether message text to be sent to the receiver from the sender has been correctly decrypted.

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Kocher with in the combination of Crepeau NPL and Rivest because it would detect errors (Kocher, Col. 28 lines 1-4). Checksums are included in stored data to detect memory corruption and write operations can be verified to detect errors.

12.5 As per claim 13, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Rivest teaches the key sharing method, comprising the step of: generating and publicizing the public information (n, k, α) by the receiver device (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34)

12.6 As per claim 14, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Kocher teaches the key sharing method, wherein, for $\alpha = \beta = 1$, α and β are deleted from the public key and the secret key, respectively (Kocher Col. 25 lines 43-58).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Kocher with in the combination of Rivest and Crepeau NPL because it would ensure content providers that unauthorized users who have lost their authorization can not access content (Kocher Col. 25 lines 43-58). Key deletion is important because when a user terminates a subscription, a password (rights key) given to a user needs to be deleted by the content providers. Otherwise the users who have lost their authorization can access content after termination.

12.7 As per claim 16, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Rivest teaches the key sharing method according to Claim 15, comprising the step of:

generating and publicizing the public information (n, k, α , a) by the receiver device (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34).

12.8 As per claim 17, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Kocher teaches the key sharing method according to Claim 15, comprising the step of, for $\alpha = \beta = 1$, deleting α and β from the public key and the secret key, respectively (Kocher Col. 25 lines 43-58).

12.9 As per claim 19, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Rivest teaches the key sharing method according to Claim 12, wherein the value of d (d>1) is variable (Rivest, Col. 4 lines 56-col. 5 lines 17).

12.10 As per claim 44, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above. In addition Kocher teaches a checksums in a secure cryptographic rights unit (Col. 28 lines 1-4) that reads on the communication system using public key cryptosystem, wherein the sender device comprises a device that generates the plaintext m so as to include check information for checking whether message text to be sent to the receiver has been correctly decrypted. The motivations for combining are the same as claim 8 above.

13. Claims 20-23, 25-28, 31, 33-35, 37-38, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent No. 4,405,829), in view of Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), and in further view of Schneier et al. (Schneier, U.S. Patent No. 5,956,404).

13.1 As per claim 22, Rivest, and Crepeau NPL teach all the subject matter as described above. In addition Rivest teaches a communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret key (p, q, β) satisfying

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β є Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

and

a public key (n, k, k(sub 0), k(sub 1), α , G, H) satisfying

- n = p^d q (d > 1 is odd)
- k, k(sub 0), k(sub 1): k is a binary length of pq, and k(sub 0), k(sub 1) are positive integers with k > k(sub 0) - k(sub 1) – 2.
- α є Z
- G: {0,1}^(k sub 0) → {0,1}^(k – (k sub 0) – 2)

H: {0,1}^(k – (k sub 0) – 2) → {0,1}^(k sub 0) (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

from the ciphertext (C, a), computing y that satisfies (y/n) = a and 0 < y < 2^(k-2) of Φ(x(sub1, p), x(sub 1, q)), Φ(-x(sub1, p), x(sub 1, q)), Φ(x(sub1, p), -x(sub 1, q)), and Φ(-x(sub1, p), -x(sub 1, q)), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more prime numbers) The motivation for combining are the same as claim 1 above;

Crepeau NPL teaches: (1) in the sender device, computing

for plain text m (m є {0,1}^(1), 1 = k – (k sub 0) – (k sub 1) – 2) and a random number r(r є {0,1}^(k sub 0))

C = x^(2nα) mod n (Crepeau NPL, page 10, 1.11);

computing

and further computing Jacobi's symbol a=(x/n), and sending ciphertext (C, a) to the receiver device (Crepeau NPL, page 5-6, 1.5); and

(2) in the receiver device, using the receiver's secret key (p, q, β) to compute

x(sub (1,p)) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

x(sub (1,q)) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Rivest, and Crepeau NPL do not explicitly teach:

X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s є {0,1}^(k – (k sub 0) –2, t є {0,1}^(k sub 0)),

Computing z = G(H(s) ⊙ t) ⊙ s,

m = { [z]^I if [z] (k sub 1) = 0^(k sub 1) "reject" otherwise
and decrypting the plaintext m by
where ([a]^k and [(a sub k)] denote first k-bits and last k-bits of a, respectively

However Schneier teaches the method of hashing the message to form message bits by padding (Schneier, Col. 3 lines 50-64) that reads on X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s є {0,1}^(k – (k sub 0) –2, t є {0,1}^(k sub 0)),

Computing z = G(H(s) ⊙ t) ⊙ s,

m = { [z]^I if [z] (k sub 1) = 0^(k sub 1) "reject" otherwise and decrypting the plaintext m by

where ([a]^k and [(a sub k)] denote first k-bits and last k-bits of a, respectively

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneier with in the combination system of Rivest and Crepeau NPL because it would ensure that the encryption becomes extremely difficult to break (Col. 3 lines 50-65). Padding or concatenating or adding more bits to the hashed message would increase the size of the bits and would create a strong audit trail for the device token. There fore it is obvious to one ordinary skilled in the art at the time the invention was made to have padding or adding more bits to the system because it would enhance security.

13.2 As per claim 25, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches a communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β є Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

Key (p, q, β) satisfying

and

a public key (n, k, k(sub 0), k(sub 1), α , G, H) satisfying

- n = p^d q (d > 1 is odd)
- k, k(sub 0), k(sub 1) є Z: k is a binary length of pq, and k(sub 0), k(sub 1) are positive integers with k > k(sub 0) - k(sub 1) – 2.
- α є Z
- α є {-1,1}
- G: {0,1}^(k sub 0) → {0,1}^(k – (k sub 0) – 2)

H: {0,1}^(k – (k sub 0) – 2) → {0,1}^(k sub 0) (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

from the ciphertext (C), computing y that satisfies (y/n) = a and 0 < y < 2^(k-2) of Φ(x(sub1, p), x(sub 1, q)), Φ(-x(sub1, p), x(sub 1, q)), Φ(x(sub1, p), -x(sub 1, q)), and Φ(-x(sub1, p), -x(sub 1, q)), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem, (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more prime numbers) The motivation for combining are the same as claim 1 above;

Crepeau NPL teaches: (1) in the sender device, computing

that satisfies a = (x/n) for plaintext m(m ϵ {0,1}^1, 1 = k-k0-k1-2) and a random number r(r ϵ {0,1}^k0) (a = (m/n) denotes Jacobi's symbol), (Crepeau NPL, page 5-6, 1.5); computing

C = x^(2nα) mod n (Crepeau NPL, page 10, 1.11);

and further sending ciphertext C to the receiver device; and

(2) in the receiver device, using the receiver's secret key (p, q, β) to

x(sub (1,p)) = C^(((p+1) β (sub q)^-1)/4) mod p, (Crepeau NPL, Page 9, 1.9)

x(sub (1,q)) = C^(((q+1) β (sub p)^-d)/4) mod q, (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Rivest, and Crepeau NPL do not explicitly teach: compute

X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s ϵ {0,1}^(k – (k sub 0) –2, t ϵ {0,1}^(k sub 0))

z = G(H(s) ⊙ t) ⊙ s,

However Schneier teaches the method of hashing the message to form message bits by padding (Schneier, Col. 3 lines 50-64) that reads on X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s ϵ {0,1}^(k – (k sub 0) –2, t ϵ {0,1}^(k sub 0))

z = G(H(s) ⊙ t) ⊙ s,

computing

m = { [z]^I if [z] (k sub 1) = 0^(k sub 1) "reject" otherwise and decrypting the plaintext m by

where ([a]^k and [(a sub k)] denote first k-bits and last k-bits of a, respectively. The rational for combining are the same as claim 22 above.

13.3 As per claim 27, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches a communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret key (p, q, β) satisfying

- p, q : prime integers, p Ξ 3 (mod 4), q Ξ 3 (mod 4)
- β ϵ Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

and

a public key (n, k, k(sub 0), k(sub 1), α , G, H) satisfying

- n = p^d q (d > 1 is odd)
- k, k(sub 0), k(sub 1) ϵ Z: k is a binary length of pq, and k(sub 0), k(sub 1) are positive integers with k > k(sub 0) - k(sub 1) – 2.
- α ϵ Z
- G: {0,1}^(k sub 0) → {0,1}^(k – (k sub 0) – 2)

- H: {0,1}^(k – (k sub 0) – 2) → {0,1}^(k sub 0) (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

sending ciphertext C to the receiver device (Rivest, Col. 4 lines 56-67);

from the ciphertext C, for y1 = Φ(x(sub1, p), x(sub 1, q)), Φ(-x(sub1, p), x(sub 1, q)), Φ(x(sub1, p), -x(sub 1, q)), and Φ(-x(sub1, p), -x(sub 1, q)), where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem (Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more prime numbers) The motivation for combining are the same as claim 1 above;

Crepeau NPL teaches: (1) in the sender device, computing

for plaintext m(m ϵ {0,1}^1, 1 = k-k0-k1-2) and a random number r(r ϵ {0,1}^k0)

C = x^(2nα) mod n (Crepeau NPL, page 10, 1.11);

computing

(2) in the receiver device, using the receiver's secret key (p, q, β) to

x(sub (1,p)) = C^(((p+1) β (sub q)^-1)/4) mod p (Crepeau NPL, Page 9, 1.9),

x(sub (1,q)) = C^(((q+1) β (sub p)^-d)/4) mod q (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Rivest, and Crepeau NPL do not explicitly teach: compute

X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s ϵ {0,1}^(k – (k sub 0) –2, t (sub i) ϵ {0,1}^(k sub 0), 1 <= i <=4)

z (sub i) = G(H(s (sub i) ⊙ t (sub i)) ⊙ s (sub i), (1<= i <= 4)

However Schneier teaches the method of hashing the message to form message bits by padding

(Schneier, Col. 3 lines 50-64) that reads on X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

When y = s||t (s є {0,1}^(k – (k sub 0) –2, t (sub i) є {0,1}^(k sub 0), 1 <= i <=4)

z (sub i) = G(H(s (sub i) ⊙ t (sub i)) ⊙ s (sub i), (1<= i <= 4)

computing

m = { [z (sub i]^i if [z (sub i)] (k sub 1) = 0^(k sub 1) "reject" otherwise and decrypting the plaintext m by

where ([a]^k and [(a sub k)] denote first k-bits and last k-bits of a, respectively. The rational for combining are the same as claim 22 above.

13.4 As per claim 34, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches a communication method using public key cryptosystem by which a sender device encrypts send data by using a receiver's public key, the method comprising key generating steps of: generating a secret

- pi : prime integers, (pi Ξ 3 (mod 4), 1 <= i<= h)
- β є Z, α β Ξ 1 (mod lcm (p - 1, q - 1))

key (pi, β) (1<=i<=h) satisfying

and

a public key (n, k, k(sub 0), k(sub 1), α , G, H) satisfying

- n = ∏^(h) (sub (i=1)) pi
- k, k(sub 0), k(sub 1) є Z: k is a binary length of pq, and k(sub 0), k(sub 1) are positive integers with k > k(sub 0) - k(sub 1) – 2.
- α є Z
- G: {0,1}^(k sub 0) → {0,1}^(k – (k sub 0))

- H: {0,1}^(k – (k sub 0)) → {0,1}^(k sub 0) (Rivest, Col. 13 lines 29-34; teaches using a modulus n which is a product of three or more primes (not necessarily distinct));

sending ciphertext C to the receiver device (Rivest, Col. 4 lines 56-67);

decrypting the plaintext m by: where Φ denotes ring isomorphism mapping from Z/(p)xZ/(q) to Z/(pq) by the Chinese remainder theorem, and ([a]^k and [(a sub k)] denote first k-bits and last k-bits of a, respectively(Rivest Col. 13 lines 29-34; teaches "Chinese remaindering" or any equivalent method to obtain the result modulo n in using a product of three or more prime numbers) The motivation for combining are the same as claim 1 above;

Crepeau NPL teaches: (1) in the sender device, computing

for plaintext m(m ϵ {0,1}^1, 1 = k-k0-k1-2) and a random number r(r ϵ {0,1}^k0)

C = x^(2nα) mod n (Crepeau NPL, page 10, 1.11);

(2) in the receiver device, using the receiver's secret key (pi, β) (1<=i<=h) to compute

x(sub (i)) = C^(((p(sub i)+1) β)/4) mod p (Crepeau NPL, Page 9, 1.9) The motivation for combining are the same as claim 1 above;

Rivest, and Crepeau NPL do not explicitly teach: compute

X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

from the ciphertext C, for 2^h pieces of {Φ(e1x1,e2x2,…,ehxh)| e1,…,eh ϵ {-1,1}}

when y1 = s(sub i)|| t(sub i) (s(sub i) ϵ {0,1}^(k sub 0), 1<=i<=2^h)

computing z (sub i) = G(H(s (sub i) ⊙ t (sub i)) ⊙ s (sub i), (1<= i <= 2^h)

m = { [z (sub i]^i if [z (sub i)] (k sub 1) = 0^(k sub 1) "reject" otherwise

However Schneier teaches the method of hashing the message to form message bits by padding

(Schneier, Col. 3 lines 50-64) that reads on X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r)))

from the ciphertext C, for 2^h pieces of {Φ(e1x1,e2x2,...,ehxh)| e1,...,eh ∈ {-1,1}}

when y1 = s(sub i)|| t(sub i) (s(sub i) ∈ {0,1}^(k sub 0), 1<=i<=2^h)

computing z (sub i) = G(H(s (sub i) ⊙ t (sub i)) ⊙ s (sub i), (1<= i <= 2^h)

m = { [z (sub i]^i if [z (sub i)] (k sub 1) = 0^(k sub 1) "reject" otherwise. The motivation for combining are the same as claim 22 above.

13.5 As per claim 20, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Schneier teaches the encryption method in public key cryptosystem, wherein one or more hash functions are publicized and the sender device comprises the steps of:

creating plaintext and random number information (Schneier, Col. 3 lines 65-col. 4 lines 26);

performing exclusive OR and data concatenation operations on the plaintext and the random number information (Schneier, Col. 7 lines 61-col. 8 lines 17);

inputting results obtained by the operations to a relevant hash function and computing the input results (Schneier, Col. 3 lines 50-64);

performing exclusive OR and data concatenation operations on the plaintext, the random number information, and the results of input to the hash function (Schneier, Col. 3 lines 65-col. 4 lines 26, col. 5 lines 42-53, col. 8 lines 9-16); and

replacing the results of the operations in a location of the plaintext m in Claim 1 or the location of a random number r, and performing encryption according to the procedure of the public key cryptosystem in Claim 1(Schneier, col. 3 lines 50-64).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneier with in the combination system of Rivest and Crepeau NPL because it would perform an encryption scheme that has a strong audit trail while not wasting a lot of the valuable message space (Schneier, Col. 3 lines 35-37). It

would provide a strong audit trail for an encryption scheme that does not waste any of the valuable message space based on the ID of the public-private key or encryption scheme.

13.6 As per claim 21, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Schneier teaches a decryption method in public key cryptosystem, for decrypting ciphertext encrypted by the method set forth according to Claim 20, the method comprising:

the decrypting step set forth in Claim 1 (Schneier, Col. 1 lines 28-65);

a step of restoring the plaintext m from the results of the logical OR and data concatenation operations performed in Claim 20 (Schneier, Col. 1 lines 28-65);

a step of verifying the validity of the procedure of the (exclusive OR and data concatenation) operations (Schneier, Col. 3 lines 50-64); and

a step of outputting decryption results (Schneier, Col. 1 lines 45-65). The rational for combining are the same as claim 20 above.

13.7 As per claim 23, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 22, comprising the step of:

generating and publicizing the public information (n, k, k0, k1, α , G, H) by the receiver device (Rivest, Col. 12 lines 59-64, col. 13 lines 19-34).

13.8 As per claim 26, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 25, comprising the step of:

generating and publicizing the public information (n, k, k0, k1, α , a , G, H) by the receiver device (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34).

13.9 As per claim 28, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 27, comprising the step of:

generating and publicizing the public information (n, k, k0, k1, α , G, H) by the receiver device (Rivest, Col. 12 lines 59-64, Col. 13 lines 29-34).

13.10 As per claim 31, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 22, wherein the value of d (d>1) is variable (Rivest, Col. 4 lines 56- col. 5 lines 17).

13.11 As per claim 33, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. An encryption method according to Claim 22, for computing ciphertext C in two different devices, comprising the steps of:

Schneier teaches the method of hashing the message to form message bits by padding (Schneier, Col. 3 lines 50-64) that reads on X = (m0^(k sub 1) ⊙ G(r)) || (r ⊙ H(m0^(k sub 1) ⊙ G(r))),

in a device 1, computing

for plaintext m(m ϵ {0,1}^1, 1 = k-k0-k1-2) and a random number r(r ϵ {0,1}^k0)

C = x^(2α) mod n (Crepeau NPL, page 10, 1.11)

and after further computing

outputting C1 to a device 2; and

in the device 2, by computing

C = C1^(n) mod n

computing the ciphertext C (Rivest Col. 4 lines 56- col. 5 lines 17). The rational for combining are the same as claim 22 above.

13.12 As per claim 35, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 34, comprising the step of:

generating and publicizing the public information (n, k, k0, k1, α , G, H) by the receiver device (Rivest, col. 12 lines 59-64, col. 13 lines 29-34).

13.13 As per claim 37, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 34, comprising the step of:

sending the plaintext or the identification information of x along with ciphertext, or creating the plaintext m or x from publicized identification information (Rivest, Abstract).

13.14 As per claim 38, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Rivest teaches the communication method using public key cryptosystem according to Claim 37, comprising the step of:

decrypting the plaintext m or the x from the ciphertext using the identification information sent along with the ciphertext or the publicized identification information (Rivest, Col. 5 lines 60-65).

13.15 As per claim 40, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above. In addition Crepeau NPL teaches the communication method using public key cryptosystem according to Claim 22, comprising the step of:

creating ciphertext C by

C = x^(2α) mod n (Crepeau NPL, Page 10, 1.11)

and creating m(sub (1,p)) and m(sub (1,q)) by

m(sub (1,p)) = C^(((p+1) β)/4) mod p (Crepeau NPL, Page 9, 1.9),

m(sub (1,q)) = C^(((q+1) β)/4) mod q (Crepeau NPL, Page 9, 1.9) The rational for combining are the same as claim 22 above.

14. Claims 7, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent 4,405,829) in view of Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), and in further view of Frank Rubin (Rubin 1994, The Quadratic and Double Quadratic Residue Ciphers (NPL) December 4, 1994).

42.1 As per claims 7, and 43, Rivest and Crepeau NPL teach all the subject matter as described above.

Rivest and Crepeau NPL do not explicitly teach the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers,

However Rubin 1999 teaches the communication method using public key cryptosystem, comprising the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers (Page 5 par. 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rubin 1994 with in the combination system of Rivest and Crepeau NPL because it would make the sequence cryptographically secure (Page 5 par. 5).

15. Claim 18, is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent 4,405,829), and Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), and in view of Kocher et al. (Kocher, U.S. Patent No. 6,289,455 B1), and in further view of Frank Rubin (Rubin 1994, The Quadratic and Double Quadratic Residue Ciphers (NPL) December 4, 1994).

43.1 As per claim 18, Rivest, Crepeau NPL, and Kocher teach all the subject matter as described above.

Rivest, Crepeau NPL, and Kocher do not explicitly teach the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers,

However Rubin 1999 teaches the step of creating the secret keys p and q by p=2p'+1 and q=2q'+1, where p' and q' are prime integers (Page 5 par. 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rubin 1994 with in the combination system of Rivest, Crepeau NPL, and Kocher because it would make the sequence cryptographically secure (Page 5 par. 5).

16. Claims 24, 29, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent No. 4,405,829), and Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), in view of Schneier et al. (Schneier, U.S. Patent No. 5,956,404), and in further view of Kocher et al. (Kocher, U.S. Patent No. 6,289,455 B1).

36.1 As per claims 24, 25, and 36 Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above.

Rivest, Crepeau NPL, and Schneier do not explicitly teach deleting α and β from the public key and the secret key, respectively,

However Kocher teaches key deletion that reads on the communication method using public key cryptosystem, comprising the step of, for $\alpha = \beta = 1$, deleting α and β from the public key and the secret key, respectively (Kocher Col. 25 lines 43-58).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Kocher with in the combination of Rivest, Crepeau NPL, and Schneier because it would ensure content providers that unauthorized users who have lost their authorization can not access content (Kocher Col. 25 lines 43-58). Key deletion is important because when a user terminates a subscription, a password (rights key) given to a user needs to be deleted by the content providers. Otherwise the users who have lost their authorization can access content after termination.

17. Claim 30, is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al. (Rivest, U.S. Patent 4,405,829), and Claude Crepeau (Crepeau NPL, Computer Science 308-547A Cryptography and Data Security 1998-1999), and in view of Schneier et al. (Schneier, U.S. Patent No. 5,956,404), and in further view of Frank Rubin (Rubin 1994, The Quadratic and Double Quadratic Residue Ciphers (NPL) December 4, 1994).

18. As per claim 30, Rivest, Crepeau NPL, and Schneier teach all the subject matter as described above.

Rivest, Crepeau NPL, and Schneier do not explicitly teach the step of creating the secret keys p and q by $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are prime integers,

However Rubin 1999 teaches the step of creating the secret keys p and q by $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are prime integers (Page 5 par. 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Rubin 1994 with in the combination system of Rivest, Crepeau NPL, and Schneier because it would make the sequence cryptographically secure, provided that the sequence is longer than the message (Page 5 par. 5).

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100